**UNITED STATES DISTRICT COURT**

**WESTERN DISTRICT OF WASHINGTON**

**SEATTLE DIVISION**

ALICIA BEREND, on behalf of herself and all others similarly situated,

Plaintiff,

v.

PROLIANCE SURGEONS, INC., P.S.,

Defendant.

Case No. 2:23-cv-01824

**CLASS ACTION COMPLAINT**

**DEMAND FOR JURY TRIAL**

Alicia Berend ("Plaintiff"), through her attorneys, individually and on behalf of all others similarly situated, brings this Class Action Complaint against Defendant Proliance Surgeons, Inc., P.S. ("Proliance Surgeons" or "Defendant"), and its present, former, or future direct and indirect parent companies, subsidiaries, affiliates, agents, and/or other related entities. Plaintiff alleges the following on information and belief—except as to her own actions, counsel's investigations, and facts of public record.



TURKE & STRAUSS LLP
613 Williamson Street, Suite 201
Madison, Wisconsin 53703-3515
TEL. 608.237.1775 • FAX 608.509.4423
www.turkestrauss.com

## NATURE OF ACTION

1. Defendant is a health care provider with over 100 locations in Washington and over 800,000 patients per year.[1] As such, Defendant stores a litany of highly sensitive personal identifiable information ("PII") and protected health information ("PHI")—together "PII/PHI"—about its current and former patients.

2. This class action arises from Defendant's *continued* failure to protect its patients' highly sensitive data.

3. Four years ago, Defendant's data systems were hacked.[2] Defendant apologized and promised to upgrade its data security.[3]

4. But that hacking was not an isolated incident—rather, it was simply part and parcel of Defendant's pattern of negligence data security.

5. Because in 2023, Defendant experienced a *second* data breach. This class action arises from that second data breach (the "Data Breach").

6. Plaintiff is a Data Breach victim, having received a breach notice—attached as Exhibit A. She brings this class action on behalf of herself, and all others harmed by Defendant's misconduct.

7. The exposure of one's PII/PHI to cybercriminals is a bell that cannot be unrung. Before this data breach, the private information of Defendant's patients was exactly that—private. Not anymore. Now, their private information is forever exposed and unsecure.

## PARTIES

8. Plaintiff, Alicia Berend, is natural person and citizen of Washington. She resides in Bellevue, Washington where she intends to remain.

---

[1] *Why Proliance Surgeons*, PROLIANCE SURGEONS, https://proliancesurgeons.com/why-proliance-surgeons/ (last visited Nov. 27, 2023).
[2] *Notice of Data Security Incident*, PROLIANCE SURGEONS, https://proliancesurgeons.com/wp-content/uploads/2020/12/Proliance-Website-Substitute-Notice.pdf (last visited Nov. 27, 2023).
[3] *Id*.



TURKE & STRAUSS LLP
613 Williamson Street, Suite 201
Madison, Wisconsin 53703-3515
TEL. 608.237.1775 • FAX 608.509.4423
www.turkestrauss.com

9. Defendant, Proliance Surgeons, Inc., P.S., is a Washington Professional Service Corporation with its principal place of business at 805 Madison Street Suite 901, Seattle, Washington 98104.

## JURISDICTION AND VENUE

10. This Court has subject matter jurisdiction over this action under the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2). The amount in controversy exceeds $5 million, exclusive of interest and costs. Members of the proposed Class are citizens of different states than Defendant. And there are over 100 putative Class members.

11. This Court has personal jurisdiction over Defendant because it is headquartered in Washington, regularly conducts business in Washington, and has sufficient minimum contacts in Washington.

12. Venue is proper in this Court because Defendant's principal office is in this District, and because a substantial part of the events, acts, and omissions giving rise to Plaintiff's claims occurred in this District.

## BACKGROUND

***Defendant Collected and Stored the PII/PHI of Plaintiff and the Class***

13. Defendant is a health care provider with over 100 locations in Washington.[4] It advertises "400 providers, including over 180 board-certified physicians."[5] And Defendant has "more than 800,000 patients every year."[6]

14. As part of its business, Defendant receives and maintains the PII/PHI of thousands of its current and former patients.

15. In collecting and maintaining the PII/PHI, Defendant agreed it would safeguard the data in accordance with its internal policies, state law, and federal law. After all, Plaintiff and Class members themselves took reasonable steps to secure their PII/PHI.

---

[4] *Why Proliance Surgeons*, PROLIANCE SURGEONS, https://proliancesurgeons.com/why-proliance-surgeons/ (last visited Nov. 27, 2023).
[5] *Id.*
[6] *Id.*



TURKE & STRAUSS LLP
613 Williamson Street, Suite 201
Madison, Wisconsin 53703-3515
TEL. 608.237.1775 • FAX 608.509.4423
www.turkestrauss.com

16. Under state and federal law, businesses like Defendant have duties to protect patients' PII/PHI and to notify them about breaches.

17. Defendant recognizes these duties. For example, in its "Privacy Policy," Defendant declares that:

a. "Proliance is committed to honoring the privacy of individuals."[7]

b. "Proliance will not disclose any personal information obtained through the Proliance site."[8]

18. Furthermore, via its "Notice of Privacy Practices," Defendant promises its patients that:

a. "Proliance Surgeons, Inc., P.S. is committed to protecting the confidentiality of your health information."[9]

b. "We are required by law to maintain the privacy of your Protected Health Information (commonly called PHI), even in electronic format, and to notify you following a breach of unsecured PHI."[10]

c. "We are also required to . . . abide by the practices of this current Notice."[11]

d. "This Notice applies to all Proliance Surgeons providers and facilities that provide health care to you."[12]

e. "Certain uses and disclosures of your protected health information will be made only with your written authorization. . . . These uses and disclosures

[7] *Disclaimer*, PROLIANCE SURGEONS, https://proliancesurgeons.com/resource/disclaimer/ (last visited Nov. 27, 2023).
[8] *Id*.
[9] *Policies*, PROLIANCE SURGEONS, https://proliancesurgeons.com/resource/policies/ (last visited Nov. 27, 2023).
[10] *Id*.
[11] *Id*.
[12] *Id*.



TURKE & STRAUSS LLP
613 Williamson Street, Suite 201
Madison, Wisconsin 53703-3515
TEL. 608.237.1775 • FAX 608.509.4423
www.turkestrauss.com

include uses and disclosures not outlined in this Notice and sale of health information."[13]

19. And again, Defendant declares that "[a]t Proliance, we're committed to maintaining the privacy of your health information."[14]

20. Elsewhere, Defendant promises that the software it uses "provides industry-leading privacy and security for our patients' data."[15]

***Defendant's Pattern of Negligence***

21. Unfortunately, Defendant's Data Breach is not an isolated incident—rather, it is simply part and parcel of Defendant's pattern of negligence data security.

22. After all, this Data Breach is the *second time* that Defendant experienced a data breach within the past several years.[16]

23. For over *seven months*—starting on November 13, 2019, and ending on June 24, 2020—Defendant's data systems were hacked.[17]

24. This data breach exposed the names, zip codes, and payment card information of Defendant's patients. [18]

25. In response, Defendant declared that "we deeply regret any worry or inconvenience that this [data breach] may cause you" and "we take information privacy and security very seriously."[19]

26. Moreover, Defendant promised that it would use "enhanced security measures to prevent similar incidents in the future."[20]

---

[13] *Id*.
[14] *Medical Records*, PROLIANCE SURGEONS, https://proliancesurgeons.com/resource/medical-records/ (last visited Nov. 27, 2023).
[15] *Phreesia FAQ*, PROLIANCE SURGEONS, https://proliancesurgeons.com/resource/phreesia-faq/ (last visited Nov. 27, 2023).
[16] *Notice of Data Security Incident*, PROLIANCE SURGEONS, https://proliancesurgeons.com/wp-content/uploads/2020/12/Proliance-Website-Substitute-Notice.pdf (last visited Nov. 27, 2023).
[17] *Id*.
[18] *Id*.
[19] *Id*.
[20] *Id*.



TURKE & STRAUSS LLP
613 Williamson Street, Suite 201
Madison, Wisconsin 53703-3515
TEL. 608.237.1775 • FAX 608.509.4423
www.turkestrauss.com

***Defendant's Data Breach***

27. On or around February 11, 2023, Defendant was hacked.[21]

28. Worryingly, Defendant has admitted that "systems and files were encrypted."[22]

29. And worse yet, Defendant has confirmed that the "unauthorized access resulted in the *removal* of a limited number of files."[23]

30. On May 24, 2023—one-hundred and two days *after* the Data Breach—Defendant realized that it had exposed its current and former patients' highly sensitive PII/PHI including:

a. names;

b. Social Security numbers;

c. dates of birth;

d. phone numbers;

e. email addresses;

f. driver license numbers;

g. usernames;

h. passwords;

i. identification information;

j. medical treatment information;

k. health insurance information; and

l. financial account numbers.[24]

31. Stunningly, Defendant appears to have delayed notifying its current and former patients until November 21, 2023—a full two-hundred and eighty-three (283) days *after* the Data Breach.[25]

---

[21] *Notice of Network Security Incident*, PROLIANCE SURGEONS, https://proliancesurgeons.com/notice-of-network-security-incident/ (last visited Nov. 27, 2023).

[22] *Id*.

[23] *Id*. (emphasis added).

[24] *Id*.

[25] *Data Breach Report*, MASS. OFFICE CONSUMER AFFAIRS BUS. REG., https://www.mass.gov/doc/data-breach-report-2023/download (last visited Nov. 27, 2023).



TURKE & STRAUSS LLP
613 Williamson Street, Suite 201
Madison, Wisconsin 53703-3515
TEL. 608.237.1775 • FAX 608.509.4423
www.turkestrauss.com

32. Thus, Defendant kept the Class in the dark—thereby depriving the Class of the opportunity to try and mitigate their injuries in a timely manner.

33. Currently, the precise number of persons injured is unclear. But upon information and belief, the size of the putative class can be ascertained from information in Defendant's custody and control. And upon information and belief, the putative class is over one hundred members—as it includes Defendant's current and former patients.

34. And when Defendant did notify Plaintiff and the Class of the Data Breach, Defendant acknowledged that the Data Breach created a present, continuing, and significant risk of suffering identity theft, warning Plaintiff and the Class:

a. "review[] financial account statements for any signs of fraudulent activity;"

b. "check[] explanation of benefits statements from health insurance providers;"

c. "plac[e] an initial 1-year 'fraud alert' on your credit files;"

d. "contact any of the three major credit bureaus;"

e. "request a 'Security Freeze' on your credit file;"

f. "file a police report in your current city of residence;"

g. "request your free credit reports by calling 1-877-322-8228 or visiting the website www.annualcreditreport.com . . . [then] review them for any discrepancies . . . [l]ook out for accounts you didn't open or inquiries from unauthorized creditors . . . [v]erify that all the information is accurate;"

h. "review the 'explanation of benefits' statements you receive from your health insurance company;"

i. "request copies of your medical records from February 11, 2023, to the present;" and



TURKE & STRAUSS LLP
613 Williamson Street, Suite 201
Madison, Wisconsin 53703-3515
TEL. 608.237.1775 • FAX 608.509.4423
www.turkestrauss.com

j. "[r]equest a current year-to-date report from your insurance company, detailing all services provided to you as a beneficiary."[26]

35. Defendant failed its duties when its inadequate security practices caused the Data Breach. In other words, Defendant's negligence is evidenced by its failure to prevent the Data Breach and stop cybercriminals from accessing the PII/PHI. And thus, Defendant caused widespread injury and monetary damages.

36. Since the breach, Defendant has "enhance[d] our cybersecurity protocols," "refine[d] our practices to enhance the security and privacy of personal and protected health information," and "implement[ed] measures to reinforce our existing cybersecurity protocols."[27]

37. But this is too little too late. Simply put, these measures—which Defendant now recognizes as necessary—should have been implemented *before* the Data Breach.

38. On information and belief, Defendant failed to adequately train its employees on reasonable cybersecurity protocols or implement reasonable security measures.

39. Further, the Notice of Data Breach shows that Defendant cannot—or will not—determine the full scope of the Data Breach, as Defendant has been unable to determine precisely what information was stolen and when.

40. Defendant has done little to remedy its Data Breach. True, Defendant has offered some Class members basic credit monitoring. But upon information and belief, such rudimentary offerings are wholly insufficient given the scope of the Data Breach.

41. Because of Defendant's Data Breach, the sensitive PII/PHI of Plaintiff and Class members was placed into the hands of cybercriminals—inflicting numerous injuries and significant damages upon Plaintiff and Class members.

[26] *Notice of Network Security Incident*, PROLIANCE SURGEONS, https://proliancesurgeons.com/notice-of-network-security-incident/ (last visited Nov. 27, 2023).
[27] *Id*.



TURKE & STRAUSS LLP
613 Williamson Street, Suite 201
Madison, Wisconsin 53703-3515
TEL. 608.237.1775 • FAX 608.509.4423
www.turkestrauss.com

42. Upon information and belief, the cybercriminals in question are particularly sophisticated. After all, the cybercriminals: (1) defeated the relevant data security systems, (2) successfully encrypted files and systems, and (3) actually *removed* sensitive files.[28]

43. And as the Harvard Business Review notes, such "[c]ybercriminals frequently use the dark web—a hub of criminal and illicit activity—to sell data from companies that they have gained unauthorized access to through credential stuffing attacks, phishing attacks, [or] hacking."[29]

44. Thus, on information and belief, Plaintiff's and the Class's stolen PII/PHI has already been published—or will be published imminently—by cybercriminals on the dark web.

***Plaintiff's Experiences and Injuries***

45. Plaintiff is a former patient of Defendant—having received medical services from approximately 2018 to February 2023.

46. Thus, Defendant obtained and maintained Plaintiff's PII/PHI.

47. As a result, Plaintiff Alicia Berend was injured by Defendant's Data Breach.

48. As a condition of receiving medical services from Defendant, Plaintiff provided Defendant with her PII/PHI. Defendant used that PII/PHI to facilitate its provision of medical services.

49. Plaintiff provided her PII/PHI to Defendant and trusted the company would use reasonable measures to protect it according to Defendant's internal policies, as well as state and federal law. Defendant obtained and continues to maintain Plaintiff's PII/PHI and has a continuing legal duty and obligation to protect that PII/PHI from unauthorized access and disclosure.

50. Plaintiff reasonably understood that a portion of the funds paid to Defendant would be used to pay for adequate cybersecurity and protection of PII/PHI.

---

[28] *Id.*

[29] Brenda R. Sharton, *Your Company's Data Is for Sale on the Dark Web. Should You Buy It Back?*, HARVARD BUS. REV. (Jan. 4, 2023) https://hbr.org/2023/01/your-companys-data-is-for-sale-on-the-dark-web-should-you-buy-it-back.



TURKE & STRAUSS LLP
613 Williamson Street, Suite 201
Madison, Wisconsin 53703-3515
TEL. 608.237.1775 • FAX 608.509.4423
www.turkestrauss.com

51. Plaintiff received a Notice of Data Breach dated November 20, 2023.

52. Thus, on information and belief, Plaintiff's PII/PHI has already been published—or will be published imminently—by cybercriminals on the dark web.

53. Through its Data Breach, Defendant compromised Plaintiff's:

a. name;

b. Social Security number;

c. date of birth;

d. phone number;

e. health insurance information;

f. medical record number;

g. medical diagnoses; and

h. medical treatment information.

54. Plaintiff has *already* suffered from identity theft and fraud. Specifically, Plaintiff has received emails indicating that someone has used her identity for various out-of-state activities—e.g., inquiring into properties in Florida.

55. Plaintiff has spent—and will continue to spend—significant time and effort monitoring her accounts to protect herself from identity theft. After all, Defendant directed Plaintiff to take those steps in its breach notice.

56. And in the aftermath of the Data Breach, Plaintiff has suffered from a spike in spam messages and phone calls.

57. Plaintiff fears for her personal financial security and worries about what information was exposed in the Data Breach.

58. Because of Defendant's Data Breach, Plaintiff has suffered—and will continue to suffer from—anxiety, sleep disruption, stress, fear, and frustration. Such injuries go far beyond allegations of mere worry or inconvenience. Rather, Plaintiff's injuries are precisely the type of injuries that the law contemplates and addresses.



TURKE & STRAUSS LLP
613 Williamson Street, Suite 201
Madison, Wisconsin 53703-3515
TEL. 608.237.1775 • FAX 608.509.4423
www.turkestrauss.com

59. Plaintiff suffered actual injury from the exposure and theft of her PII/PHI—which violates her rights to privacy.

60. Plaintiff suffered actual injury in the form of damages to and diminution in the value of her PII/PHI. After all, PII/PHI is a form of intangible property—property that Defendant was required to adequately protect.

61. Plaintiff suffered imminent and impending injury arising from the substantially increased risk of fraud, misuse, and identity theft—all because Defendant's Data Breach placed Plaintiff's PII/PHI right in the hands of criminals.

62. Because of the Data Breach, Plaintiff anticipates spending considerable amounts of time and money to try and mitigate her injuries.

63. Today, Plaintiff has a continuing interest in ensuring that her PII/PHI—which, upon information and belief, remains backed up in Defendant's possession—is protected and safeguarded from additional breaches.

***Plaintiff and the Proposed Class Face Significant Risk of Continued Identity Theft***

64. Because of Defendant's failure to prevent the Data Breach, Plaintiff and Class members suffered—and will continue to suffer—damages. These damages include, *inter alia*, monetary losses, lost time, anxiety, and emotional distress. Also, they suffered or are at an increased risk of suffering:

a. loss of the opportunity to control how their PII/PHI is used;

b. diminution in value of their PII/PHI;

c. compromise and continuing publication of their PII/PHI;

d. out-of-pocket costs from trying to prevent, detect, and recovery from identity theft and fraud;

e. lost opportunity costs and wages from spending time trying to mitigate the fallout of the Data Breach by, *inter alia*, preventing, detecting, contesting, and recovering from identify theft and fraud;

f. delay in receipt of tax refund monies;



TURKE & STRAUSS LLP
613 Williamson Street, Suite 201
Madison, Wisconsin 53703-3515
TEL. 608.237.1775 • FAX 608.509.4423
www.turkestrauss.com

g. unauthorized use of their stolen PII/PHI; and

h. continued risk to their PII/PHI—which remains in Defendant's possession—and is thus as risk for futures breaches so long as Defendant fails to take appropriate measures to protect the PII/PHI.

65. Stolen PII/PHI is one of the most valuable commodities on the criminal information black market. According to Experian, a credit-monitoring service, stolen PII/PHI can be worth up to $1,000.00 depending on the type of information obtained.

66. The value of Plaintiff and Class's PII/PHI on the black market is considerable. Stolen PII/PHI trades on the black market for years. And criminals frequently post and sell stolen information openly and directly on the "dark web"—further exposing the information.

67. It can take victims years to discover such identity theft and fraud. This gives criminals plenty of time to sell the PII/PHI far and wide.

68. One way that criminals profit from stolen PII/PHI is by creating comprehensive dossiers on individuals called "Fullz" packages. These dossiers are both shockingly accurate and comprehensive. Criminals create them by cross-referencing and combining two sources of data—first the stolen PII/PHI, and second, unregulated data found elsewhere on the internet (like phone numbers, emails, addresses, etc.).

69. The development of "Fullz" packages means that the PII/PHI exposed in the Data Breach can easily be linked to data of Plaintiff and the Class that is available on the internet.

70. In other words, even if certain information such as emails, phone numbers, or credit card numbers may not be included in the PII/PHI stolen by the cyber-criminals in the Data Breach, criminals can easily create a Fullz package and sell it at a higher price to unscrupulous operators and criminals (such as illegal and scam telemarketers) over and over. That is exactly what is happening to Plaintiff and Class members, and it is reasonable for any trier of fact, including this Court or a jury, to find that Plaintiff and other Class members' stolen PII/PHI is being misused, and that such misuse is fairly traceable to the Data Breach.



TURKE & STRAUSS LLP
613 Williamson Street, Suite 201
Madison, Wisconsin 53703-3515
TEL. 608.237.1775 • FAX 608.509.4423
www.turkestrauss.com

71. Defendant disclosed the PII/PHI of Plaintiff and Class members for criminals to use in the conduct of criminal activity. Specifically, Defendant opened up, disclosed, and exposed the PII/PHI of Plaintiff and Class members to people engaged in disruptive and unlawful business practices and tactics, including online account hacking, unauthorized use of financial accounts, and fraudulent attempts to open unauthorized financial accounts (i.e., identity fraud), all using the stolen PII/PHI.

72. Defendant's failure to promptly and properly notify Plaintiff and Class members of the Data Breach exacerbated Plaintiff and Class members' injury by depriving them of the earliest ability to take appropriate measures to protect their PII/PHI and take other necessary steps to mitigate the harm caused by the Data Breach.

***Defendant Knew—Or Should Have Known—of the Risk of a Data Breach***

73. Defendant's data security obligations were particularly important given the substantial increase in cyberattacks and/or data breaches in recent years.

74. In 2021, a record 1,862 data breaches occurred, exposing approximately 293,927,708 sensitive records—a 68% increase from 2020.[30] Of the 1,862 recorded data breaches, 330 of them, or 17.7% were in the medical or healthcare industry.[31] Those 330 reported breaches exposed nearly 30 million sensitive records (28,045,658), compared to only 306 breaches that exposed nearly 10 million sensitive records (9,700,238) in 2020.[32]

75. Indeed, cyberattacks have become so notorious that the Federal Bureau of Investigation ("FBI") and U.S. Secret Service issue warnings to potential targets, so they are aware of, and prepared for, a potential attack. As one report explained, "[e]ntities like smaller municipalities and hospitals are attractive to ransomware criminals . . . because they often have

---

[30] *See 2021 Data Breach Annual Report*, IDENTITY THEFT RESOURCE CENTER (Jan. 2022) https://notified.idtheftcenter.org/s/.

[31] *Id.*

[32] *Id.*



TURKE & STRAUSS LLP
613 Williamson Street, Suite 201
Madison, Wisconsin 53703-3515
TEL. 608.237.1775 • FAX 608.509.4423
www.turkestrauss.com

lesser IT defenses and a high incentive to regain access to their data quickly."[33]

76. In fact, according to the cybersecurity firm Mimecast, 90% of healthcare organizations experienced cyberattacks in the past year.[34]

77. Therefore, the increase in such attacks, and attendant risk of future attacks, was widely known to the public and to anyone in Defendant's industry, including Defendant.

***Defendant Failed to Follow FTC Guidelines***

78. According to the Federal Trade Commission ("FTC"), the need for data security should be factored into all business decision-making. Thus, the FTC issued numerous guidelines identifying best data security practices that businesses—like Defendant—should use to protect against unlawful data exposure.

79. In 2016, the FTC updated its publication, *Protecting Personal Information: A Guide for Business*. There, the FTC set guidelines for what data security principles and practices businesses must use.[35] The FTC declared that, *inter alia*, businesses must:

a. protect the personal customer information that they keep;

b. properly dispose of personal information that is no longer needed;

c. encrypt information stored on computer networks;

d. understand their network's vulnerabilities; and

e. implement policies to correct security problems.

80. The guidelines also recommend that businesses watch for the transmission of large amounts of data out of the system—and then have a response plan ready for such a breach.

81. Furthermore, the FTC explains that companies must:

---

[33] Ben Kochman, *FBI, Secret Service Warn of Targeted Ransomware*, LAW360 (Nov. 18, 2019), https://www.law360.com/articles/1220974/fbi-secret-service-warn-of-targeted-ransomware.

[34] *See* Maria Henriquez, *Iowa City Hospital Suffers Phishing Attack*, SECURITY MAGAZINE (Nov. 23, 2020), https://www.securitymagazine.com/articles/93988-iowa-city-hospital-suffers-phishing-attack (last visited Sept. 11, 2023).

[35] *Protecting Personal Information: A Guide for Business,* FEDERAL TRADE COMMISSION (Oct. 2016) https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf.



TURKE & STRAUSS LLP
613 Williamson Street, Suite 201
Madison, Wisconsin 53703-3515
TEL. 608.237.1775 • FAX 608.509.4423
www.turkestrauss.com

a. not maintain information longer than is needed to authorize a transaction;

b. limit access to sensitive data;

c. require complex passwords to be used on networks;

d. use industry-tested methods for security;

e. monitor for suspicious activity on the network; and

f. verify that third-party service providers use reasonable security measures.

82. The FTC brings enforcement actions against businesses for failing to protect customer data adequately and reasonably. Thus, the FTC treats the failure—to use reasonable and appropriate measures to protect against unauthorized access to confidential consumer data—as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

83. In short, Defendant's failure to use reasonable and appropriate measures to protect against unauthorized access to patients' data constitutes an unfair act or practice prohibited by Section 5 of the FTCA, 15 U.S.C. § 45.

***Defendant Failed to Follow Industry Standards***

84. Several best practices have been identified that—at a *minimum*—should be implemented by businesses like Defendant. These industry standards include: educating all employees; strong passwords; multi-layer security, including firewalls, anti-virus, and anti-malware software; encryption (making data unreadable without a key); multi-factor authentication; backup data; and limiting which employees can access sensitive data.

85. Other industry standard best practices include: installing appropriate malware detection software; monitoring and limiting the network ports; protecting web browsers and email management systems; setting up network systems such as firewalls, switches, and routers; monitoring and protection of physical security systems; protection against any possible communication system; and training staff regarding critical points.



TURKE & STRAUSS LLP
613 Williamson Street, Suite 201
Madison, Wisconsin 53703-3515
TEL. 608.237.1775 • FAX 608.509.4423
www.turkestrauss.com

86. Defendant failed to meet the minimum standards of any of the following frameworks: the NIST Cybersecurity Framework Version 1.1 (including without limitation PR.AC-1, PR.AC-3, PR.AC-4, PR.AC-5, PR.AC-6, PR.AC-7, PR.AT-1, PR.DS-1, PR.DS-5, PR.PT-1, PR.PT-3, DE.CM-1, DE.CM-4, DE.CM-7, DE.CM-8, and RS.CO-2), and the Center for Internet Security's Critical Security Controls (CIS CSC), which are all established standards in reasonable cybersecurity readiness.

87. These frameworks are applicable and accepted industry standards. And by failing to comply with these accepted standards, Defendant opened the door to the criminals—thereby causing the Data Breach.

***Defendant Violated HIPAA***

88. HIPAA circumscribes security provisions and data privacy responsibilities designed to keep patients' medical information safe. HIPAA compliance provisions, commonly known as the Administrative Simplification Rules, establish national standards for electronic transactions and code sets to maintain the privacy and security of protected health information.[36]

89. HIPAA provides specific privacy rules that require comprehensive administrative, physical, and technical safeguards to ensure the confidentiality, integrity, and security of PII/PHI and PHI is properly maintained.[37]

90. The Data Breach itself resulted from a combination of inadequacies showing Defendant failed to comply with safeguards mandated by HIPAA. Defendant's security failures include, but are not limited to:

[36] HIPAA lists 18 types of information that qualify as PHI according to guidance from the Department of Health and Human Services Office for Civil Rights, and includes, *inter alia*: names, addresses, any dates including dates of birth, Social Security numbers, and medical record numbers.

[37] *See* 45 C.F.R. § 164.306 (security standards and general rules); 45 C.F.R. § 164.308 (administrative safeguards); 45 C.F.R. § 164.310 (physical safeguards); 45 C.F.R. § 164.312 (technical safeguards).



TURKE & STRAUSS LLP
613 Williamson Street, Suite 201
Madison, Wisconsin 53703-3515
TEL. 608.237.1775 • FAX 608.509.4423
www.turkestrauss.com

a. failing to ensure the confidentiality and integrity of electronic PHI that it creates, receives, maintains and transmits in violation of 45 C.F.R. § 164.306(a)(1);

b. failing to protect against any reasonably-anticipated threats or hazards to the security or integrity of electronic PHI in violation of 45 C.F.R. § 164.306(a)(2);

c. failing to protect against any reasonably anticipated uses or disclosures of electronic PHI that are not permitted under the privacy rules regarding individually identifiable health information in violation of 45 C.F.R. § 164.306(a)(3);

d. failing to ensure compliance with HIPAA security standards by Defendant's workforce in violation of 45 C.F.R. § 164.306(a)(4);

e. failing to implement technical policies and procedures for electronic information systems that maintain electronic PHI to allow access only to those persons or software programs that have been granted access rights in violation of 45 C.F.R. § 164.312(a)(1);

f. failing to implement policies and procedures to prevent, detect, contain and correct security violations in violation of 45 C.F.R. § 164.308(a)(1);

g. failing to identify and respond to suspected or known security incidents and failing to mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity in violation of 45 C.F.R. § 164.308(a)(6)(ii);

h. failing to effectively train all staff members on the policies and procedures with respect to PHI as necessary and appropriate for staff members to carry out their functions and to maintain security of PHI in violation of 45 C.F.R. § 164.530(b) and 45 C.F.R. § 164.308(a)(5); and



TURKE & STRAUSS LLP
613 Williamson Street, Suite 201
Madison, Wisconsin 53703-3515
TEL. 608.237.1775 • FAX 608.509.4423
www.turkestrauss.com

i. failing to design, implement, and enforce policies and procedures establishing physical and administrative safeguards to reasonably safeguard PHI, in compliance with 45 C.F.R. § 164.530(c).

91. Simply put, the Data Breach resulted from a combination of insufficiencies that demonstrate Defendant failed to comply with safeguards mandated by HIPAA regulations.

## CLASS ACTION ALLEGATIONS

92. Plaintiff brings this class action under Fed. R. Civ. P. 23(a), 23(b)(2), and 23(b)(3), individually and on behalf of all members of the following class:

> All individuals residing in the United States whose PII/PHI was compromised in the Data Breach discovered by Proliance Surgeons in May 2023, including all those individuals who received notice of the breach.

93. Excluded from the Class are Defendant, its agents, affiliates, parents, subsidiaries, any entity in which Defendant has a controlling interest, any Defendant officer or director, any successor or assign, and any Judge who adjudicates this case, including their staff and immediate family.

94. Plaintiff reserves the right to amend the class definition.

95. Certification of Plaintiff's claims for class-wide treatment is appropriate because Plaintiff can prove the elements of her claims on class-wide bases using the same evidence as would be used to prove those elements in individual actions asserting the same claims.

96. Ascertainability. All members of the proposed Class are readily ascertainable from information in Defendant's custody and control. After all, Defendant already identified some individuals and sent them data breach notices.

97. Numerosity. The Class members are so numerous that joinder of all Class members is impracticable. Upon information and belief, the proposed Class includes at least one hundred members.



TURKE & STRAUSS LLP
613 Williamson Street, Suite 201
Madison, Wisconsin 53703-3515
TEL. 608.237.1775 • FAX 608.509.4423
www.turkestrauss.com

98. Typicality. Plaintiff's claims are typical of Class members' claims as each arises from the same Data Breach, the same alleged violations by Defendant, and the same unreasonable manner of notifying individuals about the Data Breach.

99. Adequacy. Plaintiff will fairly and adequately protect the proposed Class's common interests. her interests do not conflict with Class members' interests. And Plaintiff has retained counsel—including lead counsel—that is experienced in complex class action litigation and data privacy to prosecute this action on the Class's behalf.

100. Commonality and Predominance. Plaintiff's and the Class's claims raise predominantly common fact and legal questions—which predominate over any questions affecting individual Class members—for which a class wide proceeding can answer for all Class members. In fact, a class wide proceeding is necessary to answer the following questions:

a. if Defendant had a duty to use reasonable care in safeguarding Plaintiff's and the Class's PII/PHI;

b. if Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;

c. if Defendant were negligent in maintaining, protecting, and securing PII/PHI;

d. if Defendant breached contract promises to safeguard Plaintiff and the Class's PII/PHI;

e. if Defendant took reasonable measures to determine the extent of the Data Breach after discovering it;

f. if Defendant's Breach Notice was reasonable;

g. if the Data Breach caused Plaintiff and the Class injuries;

h. what the proper damages measure is; and

i. if Plaintiff and the Class are entitled to damages, treble damages, and or injunctive relief.



TURKE & STRAUSS LLP
613 Williamson Street, Suite 201
Madison, Wisconsin 53703-3515
TEL. 608.237.1775 • FAX 608.509.4423
www.turkestrauss.com

101. Superiority. A class action is superior to all other available means for the fair and efficient adjudication of this controversy. The damages or other financial detriment suffered by individual Class members are relatively small compared to the burden and expense that individual litigation against Defendant would require. Thus, it would be practically impossible for Class members, on an individual basis, to obtain effective redress for their injuries. Not only would individualized litigation increase the delay and expense to all parties and the courts, but individualized litigation would also create the danger of inconsistent or contradictory judgments arising from the same set of facts. By contrast, the class action device provides the benefits of adjudication of these issues in a single proceeding, ensures economies of scale, provides comprehensive supervision by a single court, and presents no unusual management difficulties.

## FIRST CAUSE OF ACTION
### Negligence
### (On Behalf of Plaintiff and the Class)

102. Plaintiff incorporates by reference all other paragraphs as if fully set forth herein.

103. Plaintiff and the Class entrusted their PII/PHI to Defendant on the premise and with the understanding that Defendant would safeguard their PII/PHI, use their PII/PHI for business purposes only, and/or not disclose their PII/PHI to unauthorized third parties.

104. Defendant owed a duty of care to Plaintiff and Class members because it was foreseeable that Defendant's failure—to use adequate data security in accordance with industry standards for data security—would compromise their PII/PHI in a data breach. And here, that foreseeable danger came to pass.

105. Defendant has full knowledge of the sensitivity of the PII/PHI and the types of harm that Plaintiff and the Class could and would suffer if their PII/PHI was wrongfully disclosed.

106. Defendant owed these duties to Plaintiff and Class members because they are members of a well-defined, foreseeable, and probable class of individuals whom Defendant knew or should have known would suffer injury-in-fact from Defendant's inadequate security practices. After all, Defendant actively sought and obtained Plaintiff and Class members' PII/PHI.



TURKE & STRAUSS LLP
613 Williamson Street, Suite 201
Madison, Wisconsin 53703-3515
TEL. 608.237.1775 • FAX 608.509.4423
www.turkestrauss.com

107. Defendant owed—to Plaintiff and Class members—at least the following duties to:

a. exercise reasonable care in handling and using the PII/PHI in its care and custody;

b. implement industry-standard security procedures sufficient to reasonably protect the information from a data breach, theft, and unauthorized;

c. promptly detect attempts at unauthorized access;

d. notify Plaintiff and Class members within a reasonable timeframe of any breach to the security of their PII/PHI.

108. Thus, Defendant owed a duty to timely and accurately disclose to Plaintiff and Class members the scope, nature, and occurrence of the Data Breach. After all, this duty is required and necessary for Plaintiff and Class members to take appropriate measures to protect their PII/PHI, to be vigilant in the face of an increased risk of harm, and to take other necessary steps to mitigate the harm caused by the Data Breach.

109. Defendant also had a duty to exercise appropriate clearinghouse practices to remove PII/PHI it was no longer required to retain under applicable regulations.

110. Defendant knew or reasonably should have known that the failure to exercise due care in the collecting, storing, and using of the PII/PHI of Plaintiff and the Class involved an unreasonable risk of harm to Plaintiff and the Class, even if the harm occurred through the criminal acts of a third party.

111. Defendant's duty to use reasonable security measures arose because of the special relationship that existed between Defendant and Plaintiff and the Class. That special relationship arose because Plaintiff and the Class entrusted Defendant with their confidential PII/PHI, a necessary part of obtaining services from Defendant.

112. Under the FTC Act, 15 U.S.C. § 45, Defendant had a duty to use fair and adequate computer systems and data security practices to safeguard Plaintiff and Class members' PII/PHI.



TURKE & STRAUSS LLP
613 Williamson Street, Suite 201
Madison, Wisconsin 53703-3515
TEL. 608.237.1775 • FAX 608.509.4423
www.turkestrauss.com

113. Section 5 of the FTC Act prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice by businesses, such as Defendant, of failing to use reasonable measures to protect the PII/PHI entrusted to it. The FTC publications and orders promulgated pursuant to the FTC Act also form part of the basis of Defendant's duty to protect Plaintiff and the Class members' sensitive PII/PHI.

114. Defendant violated its duty under Section 5 of the FTC Act by failing to use reasonable measures to protect PII/PHI and not complying with applicable industry standards as described in detail herein. Defendant's conduct was particularly unreasonable given the nature and amount of PII/PHI Defendant had collected and stored and the foreseeable consequences of a data breach, including, specifically, the immense damages that would result to individuals in the event of a breach, which ultimately came to pass.

115. Similarly, under HIPAA, Defendant had a duty to follow HIPAA standards for privacy and security practices—as to protect Plaintiff's and Class members' PHI.

116. Defendant violated its duty under HIPAA by failing to use reasonable measures to protect its PHI and by not complying with applicable regulations detailed *supra*. Here too, Defendant's conduct was particularly unreasonable given the nature and amount of PHI that Defendant collected and stored and the foreseeable consequences of a data breach, including, specifically, the immense damages that would result to individuals in the event of a breach, which ultimately came to pass.

117. The risk that unauthorized persons would attempt to gain access to the PII/PHI and misuse it was foreseeable. Given that Defendant hold vast amounts of PII/PHI, it was inevitable that unauthorized individuals would attempt to access Defendant's databases containing the PII/PHI —whether by malware or otherwise.

118. PII/PHI is highly valuable, and Defendant knew, or should have known, the risk in obtaining, using, handling, emailing, and storing the PII/PHI of Plaintiff and Class members' and the importance of exercising reasonable care in handling it.



TURKE & STRAUSS LLP
613 Williamson Street, Suite 201
Madison, Wisconsin 53703-3515
TEL. 608.237.1775 • FAX 608.509.4423
www.turkestrauss.com

119. Defendant improperly and inadequately safeguarded the PII/PHI of Plaintiff and the Class in deviation of standard industry rules, regulations, and practices at the time of the Data Breach.

120. Defendant breached these duties as evidenced by the Data Breach.

121. Defendant acted with wanton and reckless disregard for the security and confidentiality of Plaintiff's and Class members' PII/PHI by:

a. disclosing and providing access to this information to third parties and

b. failing to properly supervise both the way the PII/PHI was stored, used, and exchanged, and those in its employ who were responsible for making that happen.

122. Defendant breached its duties by failing to exercise reasonable care in supervising its agents, contractors, vendors, and suppliers, and in handling and securing the personal information and PII/PHI of Plaintiff and Class members which actually and proximately caused the Data Breach and Plaintiff and Class members' injury.

123. Defendant further breached its duties by failing to provide reasonably timely notice of the Data Breach to Plaintiff and Class members, which actually and proximately caused and exacerbated the harm from the Data Breach and Plaintiff and Class members' injuries-in-fact.

124. Defendant has admitted that the PII/PHI of Plaintiff and the Class was wrongfully lost and disclosed to unauthorized third persons because of the Data Breach.

125. As a direct and traceable result of Defendant's negligence and/or negligent supervision, Plaintiff and Class members have suffered or will suffer damages, including monetary damages, increased risk of future harm, embarrassment, humiliation, frustration, and emotional distress.

126. And, on information and belief, Plaintiff's PII/PHI has already been published—or will be published imminently—by cybercriminals on the dark web.

127. Defendant's breach of its common-law duties to exercise reasonable care and its failures and negligence actually and proximately caused Plaintiff and Class members actual,



TURKE & STRAUSS LLP
613 Williamson Street, Suite 201
Madison, Wisconsin 53703-3515
TEL. 608.237.1775 • FAX 608.509.4423
www.turkestrauss.com

tangible, injury-in-fact and damages, including, without limitation, the theft of their PII/PHI by criminals, improper disclosure of their PII/PHI, lost benefit of their bargain, lost value of their PII/PHI, and lost time and money incurred to mitigate and remediate the effects of the Data Breach that resulted from and were caused by Defendant's negligence, which injury-in-fact and damages are ongoing, imminent, immediate, and which they continue to face.

**SECOND CAUSE OF ACTION**
**Breach of Implied Contract**
**(On Behalf of Plaintiff and the Class)**

128. Plaintiff incorporates by reference all other paragraphs as if fully set forth herein.

129. Plaintiff and Class members were required to provide their PII/PHI to Defendant as a condition of receiving medical services provided by Defendant. Plaintiff and Class members provided their PII/PHI to Defendant or its third-party agents in exchange for Defendant's medical services.

130. Plaintiff and Class members reasonably understood that a portion of the funds they paid Defendant would be used to pay for adequate cybersecurity measures.

131. Plaintiff and Class members reasonably understood that Defendant would use adequate cybersecurity measures to protect the PII/PHI that they were required to provide based on Defendant's duties under state and federal law and its internal policies.

132. Plaintiff and the Class members accepted Defendant's offers by disclosing their PII/PHI to Defendant or its third-party agents in exchange for medical services.

133. In turn, and through internal policies, Defendant agreed to protect and not disclose the PII/PHI to unauthorized persons.

134. In its various policies, Defendant represented that they had a legal duty to protect Plaintiff's and Class Member's PII/PHI.

135. Implicit in the parties' agreement was that Defendant would provide Plaintiff and Class members with prompt and adequate notice of all unauthorized access and/or theft of their PII/PHI.



TURKE & STRAUSS LLP
613 Williamson Street, Suite 201
Madison, Wisconsin 53703-3515
TEL. 608.237.1775 • FAX 608.509.4423
www.turkestrauss.com

136. After all, Plaintiff and Class members would not have entrusted their PII/PHI to Defendant in the absence of such an agreement with Defendant.

137. Plaintiff and the Class fully performed their obligations under the implied contracts with Defendant.

138. The covenant of good faith and fair dealing is an element of every contract. Thus, parties must act with honesty in fact in the conduct or transactions concerned. Good faith and fair dealing, in connection with executing contracts and discharging performance and other duties according to their terms, means preserving the spirit—and not merely the letter—of the bargain. In short, the parties to a contract are mutually obligated to comply with the substance of their contract in addition to its form.

139. Subterfuge and evasion violate the duty of good faith in performance even when an actor believes their conduct to be justified. Bad faith may be overt or consist of inaction. And fair dealing may require more than honesty.

140. Defendant materially breached the contracts it entered with Plaintiff and Class members by:

a. failing to safeguard their information;

b. failing to notify them promptly of the intrusion into its computer systems that compromised such information.

c. failing to comply with industry standards;

d. failing to comply with the legal obligations necessarily incorporated into the agreements; and

e. failing to ensure the confidentiality and integrity of the electronic PII/PHI that Defendant created, received, maintained, and transmitted.

141. In these and other ways, Defendant violated its duty of good faith and fair dealing.

142. Defendant's material breaches were the direct and proximate cause of Plaintiff's and Class members' injuries (as detailed *supra*).



TURKE & STRAUSS LLP
613 Williamson Street, Suite 201
Madison, Wisconsin 53703-3515
TEL. 608.237.1775 • FAX 608.509.4423
www.turkestrauss.com

143. And, on information and belief, Plaintiff's PII/PHI has already been published—or will be published imminently—by cybercriminals on the dark web.

144. Plaintiff and Class members performed as required under the relevant agreements, or such performance was waived by Defendant's conduct.

## THIRD CAUSE OF ACTION
**Breach of Fiduciary Duty**
**(On Behalf of Plaintiff and the Class)**

145. Plaintiff incorporates by reference all other paragraphs as if fully set forth herein.

146. Given the relationship between Defendant and Plaintiff and Class members, where Defendant became guardian of Plaintiff's and Class members' PII/PHI, Defendant became a fiduciary by its undertaking and guardianship of the PII/PHI, to act primarily for Plaintiff and Class members, (1) for the safeguarding of Plaintiff and Class members' PII/PHI; (2) to timely notify Plaintiff and Class members of a Data Breach and disclosure; and (3) to maintain complete and accurate records of what information (and where) Defendant did and does store.

147. Defendant has a fiduciary duty to act for the benefit of Plaintiff and Class members upon matters within the scope of Defendant's relationship with them—especially to secure their PII/PHI.

148. Because of the highly sensitive nature of the PII/PHI, Plaintiff and Class members would not have entrusted Defendant, or anyone in Defendant's position, to retain their PII/PHI had they known the reality of Defendant's inadequate data security practices.

149. Defendant breached its fiduciary duties to Plaintiff and Class members by failing to sufficiently encrypt or otherwise protect Plaintiff's and Class members' PII/PHI.

150. Defendant also breached its fiduciary duties to Plaintiff and Class members by failing to diligently discover, investigate, and give notice of the Data Breach in a reasonable and practicable period.



TURKE & STRAUSS LLP
613 Williamson Street, Suite 201
Madison, Wisconsin 53703-3515
TEL. 608.237.1775 • FAX 608.509.4423
www.turkestrauss.com

151. As a direct and proximate result of Defendant's breach of its fiduciary duties, Plaintiff and Class members have suffered and will continue to suffer numerous injuries (as detailed *supra*).

**FOURTH CAUSE OF ACTION**
**Invasion of Privacy**
**(On Behalf of Plaintiff and the Class)**

152. Plaintiff incorporates by reference all other paragraphs as if fully set forth herein.

153. Plaintiff and the Class had a legitimate expectation of privacy regarding their highly sensitive and confidential PII/PHI and were accordingly entitled to the protection of this information against disclosure to unauthorized third parties.

154. Defendant owed a duty to its current and former patients, including Plaintiff and the Class, to keep this information confidential.

155. The unauthorized acquisition (i.e., theft) by a third party of Plaintiff and Class members' PII/PHI is highly offensive to a reasonable person.

156. The intrusion was into a place or thing which was private and entitled to be private. Plaintiff and the Class disclosed their sensitive and confidential information to Defendant, but did so privately, with the intention that their information would be kept confidential and protected from unauthorized disclosure. Plaintiff and the Class were reasonable in their belief that such information would be kept private and would not be disclosed without their authorization.

157. The Data Breach constitutes an intentional interference with Plaintiff's and the Class's interest in solitude or seclusion, either as to their person or as to their private affairs or concerns, of a kind that would be highly offensive to a reasonable person.

158. Defendant acted with a knowing state of mind when it permitted the Data Breach because it knew its information security practices were inadequate.

159. Defendant acted with a knowing state of mind when it failed to notify Plaintiff and the Class in a timely fashion about the Data Breach, thereby materially impairing their mitigation efforts.



TURKE & STRAUSS LLP
613 Williamson Street, Suite 201
Madison, Wisconsin 53703-3515
TEL. 608.237.1775 • FAX 608.509.4423
www.turkestrauss.com

160. Acting with knowledge, Defendant had notice and knew that its inadequate cybersecurity practices would cause injury to Plaintiff and the Class.

161. As a proximate result of Defendant's acts and omissions, the private and sensitive PII/PHI of Plaintiff and the Class were stolen by a third party and is now available for disclosure and redisclosure without authorization, causing Plaintiff and the Class to suffer damages (as detailed *supra*).

162. And, on information and belief, Plaintiff's PII/PHI has already been published—or will be published imminently—by cybercriminals on the dark web.

163. Unless and until enjoined and restrained by order of this Court, Defendant's wrongful conduct will continue to cause great and irreparable injury to Plaintiff and the Class since their PII/PHI are still maintained by Defendant with their inadequate cybersecurity system and policies.

164. Plaintiff and the Class have no adequate remedy at law for the injuries relating to Defendant's continued possession of their sensitive and confidential records. A judgment for monetary damages will not end Defendant's inability to safeguard the PII/PHI of Plaintiff and the Class.

165. In addition to injunctive relief, Plaintiff, on behalf of herself and the other Class members, also seeks compensatory damages for Defendant's invasion of privacy, which includes the value of the privacy interest invaded by Defendant, the costs of future monitoring of their credit history for identity theft and fraud, plus prejudgment interest and costs.

## FIFTH CAUSE OF ACTION
### Unjust Enrichment
### (On Behalf of Plaintiff and the Class)

166. Plaintiff incorporates by reference all other paragraphs as if fully set forth herein.

167. This claim is pleaded in the alternative to the breach of implied contract claim.

168. Plaintiff and Class members conferred a benefit upon Defendant. After all, Defendant benefitted from using their payment and PII/PHI to provide medical services. Furthermore, Defendant benefitted from using their PII/PHI to collect payment.



TURKE & STRAUSS LLP
613 Williamson Street, Suite 201
Madison, Wisconsin 53703-3515
TEL. 608.237.1775 • FAX 608.509.4423
www.turkestrauss.com

169. Defendant appreciated or had knowledge of the benefits it received from Plaintiff and Class members (or their third-party agents). And Defendant benefited from receiving Plaintiff's and Class members' payment and PII/PHI, as they was used to provide medical services.

170. Plaintiff and Class members reasonably understood that Defendant would use adequate cybersecurity measures to protect the PII/PHI that they were required to provide based on Defendant's duties under state and federal law and its internal policies.

171. Defendant enriched itself by saving the costs they reasonably should have expended on data security measures to secure Plaintiff's and Class members' PII/PHI.

172. Instead of providing a reasonable level of security, or retention policies, that would have prevented the Data Breach, Defendant instead calculated to avoid its data security obligations at the expense of Plaintiff and Class members by utilizing cheaper, ineffective security measures. Plaintiff and Class members, on the other hand, suffered as a direct and proximate result of Defendant's failure to provide the requisite security.

173. Under principles of equity and good conscience, Defendant should not be permitted to retain the full value of Plaintiff's and Class members' PII/PHI and payment because Defendant failed to adequately protect their PII/PHI.

174. Plaintiff and Class members have no adequate remedy at law.

175. Defendant should be compelled to disgorge into a common fund—for the benefit of Plaintiff and Class members—all unlawful or inequitable proceeds that it received because of its misconduct.

## SIXTH CAUSE OF ACTION
**Violation of the Washington Consumer Protection Act**
**RCW 19.86.010, *et seq*.**
**(On Behalf of Plaintiff and the Class)**

176. Plaintiff incorporates by reference all other paragraphs as if fully set forth herein.



TURKE & STRAUSS LLP
613 Williamson Street, Suite 201
Madison, Wisconsin 53703-3515
TEL. 608.237.1775 • FAX 608.509.4423
www.turkestrauss.com

177. The Washington State Consumer Protection Act, RCW 19.86.020 (the "CPA") prohibits any "unfair or deceptive acts or practices" in the conduct of any trade or commerce as those terms are described by the CPA and relevant case law.

178. Defendant is a "person" as described in RWC 19.86.010(1).

179. Defendant engages in "trade" and "commerce" as described in RWC 19.86.010(2) in that they engage in the sale of services and commerce directly and indirectly affecting the people of the State of Washington.

180. By virtue of the above-described wrongful actions, inaction, omissions, and want of ordinary care that directly and proximately caused the Data Breach, Defendant engaged in unlawful, unfair and fraudulent practices within the meaning, and in violation of, the CPA, in that Defendant's practices were injurious to the public interest because they injured other persons, had the capacity to injure other persons, and have the capacity to injure other persons.

181. Defendant's failure to safeguard the PII/PHI exposed in the Data Breach constitutes an unfair act that offends public policy.

182. Defendant's failure to safeguard the PII/PHI compromised in the Data Breach caused substantial injury to Plaintiff and Class Members. Defendant's failure is not outweighed by any countervailing benefits to consumers or competitors, and it was not reasonably avoidable by consumers.

183. Defendant's failure to safeguard the PII/PHI disclosed in the Data Breach, and its failure to provide timely and complete notice of that Data Breach to the victims, is unfair because these acts and practices are immoral, unethical, oppressive, and/or unscrupulous.

184. In the course of conducting their business, Defendant committed "unfair or deceptive acts or practices" by, *inter alia*, knowingly failing to design, adopt, implement, control, direct, oversee, manage, monitor and audit appropriate data security processes, controls, policies, procedures, protocols, and software and hardware systems to safeguard and protect Plaintiff's and Class Members' PII/PHI, and violating the common law alleged herein in the process. Plaintiff and Class Members reserve the right to allege other violations of law by Defendant constituting



TURKE & STRAUSS LLP
613 Williamson Street, Suite 201
Madison, Wisconsin 53703-3515
TEL. 608.237.1775 • FAX 608.509.4423
www.turkestrauss.com

other unlawful business acts or practices. As described above, Defendant's wrongful actions, inaction, omissions, and want of ordinary care are ongoing and continue to this date.

185. Defendant also violated the CPA by failing to timely notify, and by concealing from Plaintiff and Class Members, information regarding the unauthorized release and disclosure of their PII/PHI. If Plaintiff and Class Members had been notified in an appropriate fashion, and had the information not been hidden from them, they could have taken precautions to safeguard and protect their PII/PHI and identities.

186. Defendant's above-described wrongful actions, inaction, omissions, want of ordinary care, misrepresentations, practices, and non-disclosures also constitute "unfair or deceptive acts or practices" in violation of the CPA in that Defendant's wrongful conduct is substantially injurious to other persons, had the capacity to injure other persons, and has the capacity to injure other persons.

187. The gravity of Defendant's wrongful conduct outweighs any alleged benefits attributable to such conduct. There were reasonably available alternatives to further Defendant's legitimate business interests other than engaging in the above-described wrongful conduct.

188. Defendant's unfair or deceptive acts or practices occurred in its trade or business and have and injured and are capable of injuring a substantial portion of the public. Defendant's general course of conduct as alleged herein is injurious to the public interest, and the acts complained of herein are ongoing and/or have a substantial likelihood of being repeated.

189. As a direct and proximate result of Defendant's above-described wrongful actions, inaction, omissions, and want of ordinary care that directly and proximately caused the Data Breach and their violations of the CPA, Plaintiff and Class Members have suffered, and will continue to suffer, economic damages and other injury and actual harm in the form of, *inter alia*, (1) an imminent, immediate and the continuing increased risk of identity theft, identity fraud—risks justifying expenditures for protective and remedial services for which they are entitled to compensation; (2) invasion of privacy; (3) breach of the confidentiality of their PII/PHI; (5) deprivation of the value of their PII/PHI, for which there is a well-established national and



TURKE & STRAUSS LLP
613 Williamson Street, Suite 201
Madison, Wisconsin 53703-3515
TEL. 608.237.1775 • FAX 608.509.4423
www.turkestrauss.com

international market; and/or (6) the financial and temporal cost of monitoring credit, monitoring financial accounts, and mitigating damages.

190. Unless restrained and enjoined, Defendant will continue to engage in the above-described wrongful conduct and more data breaches will occur. Plaintiff, therefore, on behalf of themselves and the Class, seek restitution and an injunction prohibiting Defendant from continuing such wrongful conduct, and requiring Defendant to design, adopt, implement, control, direct, oversee, manage, monitor and audit appropriate data security processes, controls, policies, procedures protocols, and software and hardware systems to safeguard and protect the PII/PHI entrusted to it.

191. Plaintiff, on behalf of themselves and Class Members, also seek to recover actual damages sustained by each Class Member together with the costs of the suit, including reasonable attorney fees. In addition, Plaintiff, on behalf of themselves and Class Members, request that this Court use its discretion, pursuant to RCW 19.86.090, to increase the damages award for each Class Member by three times the actual damages sustained not to exceed $25,000.00 per Class Member.

## SEVENTH CAUSE OF ACTION
**Violation of the Washington Data Breach Disclosure Law**
**RCW 19.255.005, *et seq*.**
**(On Behalf of Plaintiff and the Class)**

192. Plaintiff incorporates by reference all other paragraphs as if fully set forth herein.

193. Under RCW § 19.255.010(2), "[a]ny person or business that maintains computerized data that includes personal information that the person or business does not own shall notify the owner or licensee of the information of any breach of the security of the data immediately following discovery, if the personal information was, or is reasonably believed to have been, acquired by an unauthorized person."

194. Upon information and belief, this statute applies to Defendant because Defendant does not own nor license the PII/PHI in question. Instead, the owners and/or licensees of the PII/PHI are Plaintiff and the Class.



TURKE & STRAUSS LLP
613 Williamson Street, Suite 201
Madison, Wisconsin 53703-3515
TEL. 608.237.1775 • FAX 608.509.4423
www.turkestrauss.com

195. Here, the Data Breach led to "unauthorized acquisition of computerized data that compromise[d] the security, confidentiality, [and] integrity of personal information maintained by" Defendant, leading to a "breach of the security of [Defendant's] systems," as defined by RCW § 19.255.010.

196. Defendant failed to disclose that the PII/PHI—of Plaintiffs and Class Members—that had been compromised "immediately" upon discovery, and thus unreasonably delayed informing Plaintiffs and the proposed Class about the Data Breach.

197. In fact, Defendant appears to have delayed notifying its current and former patients until November 21, 2023—a full two-hundred and eighty-three (283) days *after* the Data Breach.

198. Thus, Defendant violated the Washington Data Breach Disclosure Law.

## EIGHTH CAUSE OF ACTION
**Violation of the Washington Uniform Health Care Information Act (UHCIA)**
**RCW 70.02.005, *et seq*.**
**(On Behalf of Plaintiff and the Class)**

199. Plaintiff incorporates by reference all other paragraphs as if fully set forth herein.

200. UHCIA declares that:

a. "Health care information is personal and sensitive information that if improperly used or released may do significant harm to a patient's interests in privacy, health care, or other interests." § 70.02.005(1).

b. "In order to retain the full trust and confidence of patients, health care providers have an interest in assuring that health care information is not improperly disclosed and in having clear and certain rules for the disclosure of health care information." § 70.02.005(3).

c. "It is the public policy of this state that a patient's interest in the proper use and disclosure of the patient's health care information survives even when the information is held by persons other than health care providers." § 70.02.005(4).



TURKE & STRAUSS LLP
613 Williamson Street, Suite 201
Madison, Wisconsin 53703-3515
TEL. 608.237.1775 • FAX 608.509.4423
www.turkestrauss.com

201. Here, Defendant is a "health care provider" because Defendant "is licensed, certified, registered, or otherwise authorized by the law of this state to provide health care in the ordinary course of business or practice of a profession." § 70.02.010(19).

202. Under § 70.02.020, "a health care provider, an individual who assists a health care provider in the delivery of health care, or an agent and employee of a health care provider may not disclose health care information about a patient to any other person without the patient's written authorization."

203. Here, Defendant violated UHCIA because Defendant—via its Data Breach—disclosed health care information to third parties without patient authorization.

## NINTH CAUSE OF ACTION
### Declaratory Judgment
### (On Behalf of Plaintiff and the Class)

204. Plaintiff incorporates by reference all other paragraphs as if fully set forth herein.

205. Under the Declaratory Judgment Act, 28 U.S.C. §§ 2201, *et seq*., this Court is authorized to enter a judgment declaring the rights and legal relations of the parties and to grant further necessary relief. The Court has broad authority to restrain acts, such as those alleged herein, which are tortious and unlawful.

206. In the fallout of the Data Breach, an actual controversy has arisen about Defendant's various duties to use reasonable data security. On information and belief, Plaintiff alleges that Defendant's actions were—and *still* are—inadequate and unreasonable. And Plaintiff and Class members continue to suffer injury from the ongoing threat of fraud and identity theft.

207. Given its authority under the Declaratory Judgment Act, this Court should enter a judgment declaring, among other things, the following:

a. Defendant owed—and continues to owe—a legal duty to use reasonable data security to secure the data entrusted to it;

b. Defendant has a duty to notify impacted individuals of the Data Breach under the common law and Section 5 of the FTC Act;



TURKE & STRAUSS LLP
613 Williamson Street, Suite 201
Madison, Wisconsin 53703-3515
TEL. 608.237.1775 • FAX 608.509.4423
www.turkestrauss.com

c. Defendant breached, and continues to breach, its duties by failing to use reasonable measures to the data entrusted to it; and

d. Defendant breaches of its duties caused—and continues to cause—injuries to Plaintiff and Class members.

208. The Court should also issue corresponding injunctive relief requiring Defendant to use adequate security consistent with industry standards to protect the data entrusted to it.

209. If an injunction is not issued, Plaintiff and the Class will suffer irreparable injury and lack an adequate legal remedy if Defendant experiences a second data breach.

210. And if a second breach occurs, Plaintiff and the Class will lack an adequate remedy at law because many of the resulting injuries are not readily quantified in full and they will be forced to bring multiple lawsuits to rectify the same conduct. Simply put, monetary damages—while warranted for out-of-pocket damages and other legally quantifiable and provable damages—cannot cover the full extent of Plaintiff and Class members' injuries.

211. If an injunction is not issued, the resulting hardship to Plaintiff and Class members far exceeds the minimal hardship that Defendant could experience if an injunction is issued.

212. An injunction would benefit the public by preventing another data breach—thus preventing further injuries to Plaintiff, Class members, and the public at large.

**PRAYER FOR RELIEF**

Plaintiff and Class members respectfully request judgment against Defendant and that the Court enter an order:

A. Certifying this case as a class action on behalf of Plaintiff and the proposed Class, appointing Plaintiff as class representative, and appointing her counsel to represent the Class;

B. Awarding declaratory and other equitable relief as necessary to protect the interests of Plaintiff and the Class;

C. Awarding injunctive relief as necessary to protect the interests of Plaintiff and the Class;



TURKE & STRAUSS LLP
613 Williamson Street, Suite 201
Madison, Wisconsin 53703-3515
TEL. 608.237.1775 • FAX 608.509.4423
www.turkestrauss.com

D. Awarding Plaintiff and the Class damages including applicable compensatory, exemplary, punitive damages, and statutory damages, as allowed by law;

E. Awarding restitution and damages to Plaintiff and the Class in an amount to be determined at trial;

F. Awarding attorneys' fees and costs, as allowed by law;

G. Awarding prejudgment and post-judgment interest, as provided by law;

H. Granting Plaintiff and the Class leave to amend this complaint to conform to the evidence produced at trial; and

I. Granting other relief that this Court finds appropriate.

**DEMAND FOR JURY TRIAL**

Plaintiff demands a jury trial for all claims so triable.

Dated: November 27, 2023

By: */s/ Samuel J. Strauss*

Samuel J. Strauss, WSBA #46971
TURKE & STRAUSS LLP
613 Williamson St., Suite 201
Madison, Wisconsin 53703-3515
Telephone: (608) 237-1775
Facsimile: (608) 509 4423
sam@turkestrauss.com

*Attorneys for Plaintiff and the Proposed Class*